Electronic Version
Stylesheet Version v1.1.1

Description

METHOD AND SYSTEM FOR MANAGING PRIVACY PREFERENCES

BACKGROUND OF INVENTION

[0001] The present invention relates to privacy of personal and other restricted information and more particularly to a method and system for managing privacy preferences attached to federated content or the like.

[0002] Today, web or Internet users are constantly faced with the decision of whether and under what circumstances to disclose personal information. Virtually any information including personal or private information is being stored electronically and may be accessed via electronic means. This makes managing access to personal or private information or other information to which one may desire to limit or restrict access a challenge. Authors who create papers or other works may have particular preferences in whether their personal information or to what extent such information is available when such papers or works are

available via a network, such as the Internet. Such works or papers may be stored or reside as content objects in federated content repositories. Federated content may be maintained and owned by the contributing organization that initially authored or made available the content. As content is exchanged among business entities, privacy policies or preferences of federated content owners or authors needs to be honored and access controlled or managed, preferably automatically.

SUMMARY OF INVENTION

[0003] In accordance with an embodiment of the present invention, a method for managing privacy preferences or access to restricted information may include tagging restricted or personal information. The method may also include defining a content object with a link to the restricted or personal information.

[0004] In accordance with another embodiment of the present invention, a method for managing privacy or access to restricted information may include collecting a content object responsive to a request. The method may also include accessing privacy preferences of an author or other restriction preferences and comparing the privacy preferences or other restriction preferences to a content

provider's or web site's policies.

[0005] In accordance with another embodiment of the present invention, a system for managing privacy preferences or access to restricted information may include a server to collect a content object in response to a request. The system may also include a privacy function operable on the server to access privacy preferences of an author of the content object or other restriction preferences. Means may also be included for comparing the privacy preferences or other restriction preferences to policies of a content provider or web site.

[0006] In accordance with another embodiment of the present invention, a method for making a system for managing privacy preferences or access to restricted information may include providing a server to collect a content object in response to a request. A privacy function may be provided that is operable on the server to access privacy preferences of an author or provider of the content object or other restriction preferences. The method may also include providing means for comparing the privacy preferences or other restriction preferences to a content provider's or web site's policies.

[0007] In accordance with another embodiment of the present in-

vention, a computer-readable medium having computer-executable instruction for performing a method including collecting a content object responsive to a request. The method may also include accessing privacy preferences of an author of the content object or other restriction preferences. The method may further include comparing the privacy preferences or other restriction preferences to policies of a content provider or web page.

Brief Description of Drawings

[0008] Figure 1 is a flow chart of a method for automatically managing privacy preferences or access to restricted information in accordance with an embodiment of the present invention.

[0009] Figure 2 is an example of a content object illustrating how personal identification information may be identified or tagged in accordance with an embodiment of the present invention.

[0010] Figures 3A and 3B (collectively Figure 3) are a flow chart of a method for automatically managing privacy preferences or access to restricted information in accordance with another embodiment of the present invention.

[0011] Figures 4A and 4B illustrate an example of a system and a sequence of operations that may be carried out by the

system for automatically managing privacy preferences or access to restricted information in accordance with an embodiment of the present invention.

Detailed Description

[0012] The following detailed description of preferred embodiments refers to the accompanying drawings which illustrate specific embodiments of the invention. Other embodiments having different structures and operations do not depart from the scope of the present invention.

[0013] Figure 1 is a flow chart of a method 100 for automatically managing privacy preferences or access to restricted information in accordance with an embodiment of the present invention. In block 102, personal identifiable information (PII), privacy information or other information to which access is intended to be restricted or limited may be tagged or otherwise identified in a content object. The content object may be a white paper, case study, press release, news article or any sort of document, viewable article or other work. Figure 2 is an example of a content object 200 illustrating how personal identification information (PII) may be identified or may be tagged in accordance with an embodiment of the present invention. The example of the content object 200 illustrated in Figure 2

is a white paper but may be any sort of document or viewable article as previously listed. The taxonomy of the white paper 200 may include different component parts, such as a title 202, subtitle 204, abstract 206, description 208, author PII 210 and body 212. The author PII 210 may include different components, such as first name 214, last name 216 and other restricted information 218, such as contact information, address, curriculum vitae or the like. As an example, the content object may be represented via a mark-up language, such as Extensible Markup Language (XML) or other representation that may be effectively stored and presented electronically on the Internet or other network as shown below. The XML schema may include Platform for Privacy Preferences Project (P3P) syntax that indicate elements that are considered PII (author complex type).

[0014]

```
p3pwhitepaper.xsd
<xsd:schema xmlns:xsd ="http://www.w3.org/2001/XMLSchema"
      xmlns:p3p ="http://www.w3.org/2001/12/P3Pv1">
 <xsd:annotation>
  <xsd:documentation xml:lang="en">
   Whitepaper schema content object
  </xsd:documentation>
 </xsd:annotation>

 <xsd:element name="whitePaper" type="WhitePaperType"/>
 <xsd:complexType name="WhitePaperType ">
  <xsd:sequence>
   <xsd:element name="title" type="xsd:string"/>
   <xsd:element name="subtitle" type="xsd:string"/>
   <xsd:element name="abstract" type="xsd:string"/>
   <xsd:element name="description"  type="xsd:string"/>
   <xsd:element name="author"  type="Author"/>
   <xsd:element name="body"  type="xsd:string"/>
  </xsd:sequence>
  <xsd:attribute name="whitePaperDate" type="xsd:date"/>
 </xsd:complexType>

 <xsd:complexType name="Author">
  <xsd:sequence>
    <xsd:element name="fname"   type="p3p:user.name.personname.given"/>
    <xsd:element name="lname"   type="p3p:user.name.personname.family"/>
   <xsd:element name="jobtitle"   type="p3p:user.jobtitle"/>
    <xsd:element name="officeName"   type="p3p: business.name "/>
    <xsd:element name="officeEmail"   type="p3p: business.contact-info.online.email "/>
    <xsd:element name="officephone"   type="p3p:business.contact-
info.telecom.telephone.intcode "/>
    <xsd:element name="officestreet" type="p3p: business.contact-info.postal.street "/>
   <xsd:element name="officecity"   type="p3p: business.contact-info.postal.city "/>
   <xsd:element name="officestate"  type="p3p: business.contact-info.postal.stateprov "/>
   <xsd:element name="officezip"    type="p3p: business.contact-info.postal.postalcode "/>
  </xsd:sequence>
 </xsd:complexType>
</xsd:schema>
```

[0015] In this example of a content object, the Personal Identifiable Information (PII) may be tagged or identified by a "type = p3p" type tag. While PII may be tagged or identified in this manner, any sort of information desired to be restricted or kept confidential may be identified or tagged with a p3p syntax or the like.

[0016] In block 104 of Figure 1, the content object may be defined as an XML document or document accessible or presentable via the Internet, web or the like, with an xLink at-

tribute or similar link to personal or restricted information. An example of the content object defined in an XML file with an xLink attribute to the author complex type elements is illustrated below. The xLink couples the author's P3P privacy preferences to the actual PII content.

[0017]

p3pwhitepaper.xml

```
<?xml version ="1.0"?>
<whitePaper xmlns:p3p ="http://www.w3.org/2001/12/P3Pv1"
            xmlns:xlink ="http://www.w3.org/1999/xlink">
  <title "Title of the whitepaper"/>
  <subtitle "Subtitle of the whitepaper"/>
  <abstract "Abstract of the whitepaper"/>
  <description "Description of the whitepaper"/>
  <author xlink:type = "simple"
          xlink: href = "www.ibm.com/content_preferences/contnet_privacy_prefs.xml">
      <p3p:fname "Fonda"/>
      < p3p:lname "Daniels"/>
      <p3p:jobtitle "Competitive Intelligence"/>
      <p3p:officeName "IBM"/>
      <p3p:officeEmail "fondad@us.ibm.com"/>
      <p3p:officephone "919-224-1117"/>
      <p3p:officestreet "3901 South Miami"/>
      <p3p:officecity "Durham"/>
      <p3p:officestate "NC"/>
      <p3p:officezip "27709"/>
  </author>
</whitepaper>
```

[0018] In block 106, the content object may be stored and access may be provided on request. In block 108, the personal identifiable information or other restricted information may also be stored in a different storage location or device. Access to the personal identifiable information or restricted information may be provided via an xLink, as illustrated above, or via some other secure arrangement or

means.

[0019] Figures 3A and 3B (collectively Figure 3) are a flow chart of a method 300 for automatically managing privacy preferences or access to restricted information in accordance with another embodiment of the present invention. In block 302, a request may be received. The request may be received by a web server or like as will be discussed in more detail herein. The request may be for information, such as a white paper or other content object similar to the examples previously described. In block 304, sources that may contain the requested content object may be interrogated in response to the request. Content objects responsive to the request may be collected. As described in more detail herein, a collection function, such as a collection servlet operable on a web server, may interrogate the content sources and collect content objects responsive to the request.

[0020] In block 306, any content objects collected in block 304 may be distributed or transmitted by the collection function to a privacy function or P3P servlet. In block 308, the content object may be parsed to provide access to privacy preferences of the author of the content object or other restriction preferences. The privacy function or P3P servlet

may parse the privacy preferences or other restriction preferences. The privacy preferences or restriction preferences may be accessed or located via an xLink associated with each of the components of the personal identifiable information or a similar link or access mechanism.

[0021] In block 310, the author's privacy preferences or other restriction preferences may be compared to the web site's or content provider's policies. The privacy function or P3P servlet may compare the privacy preferences or other restriction preferences to the web site's or service provider's policies. In block 312 (Figure 3B), a determination may be made if the privacy or restriction preferences are consistent when compared to the policies of the web site or service provider. If the preferences and policies are consistent in block 312, the method 300 may advance to block 314 where the original content object may be returned to the collection function or servlet for distribution to the requester. If the preferences and policies are inconsistent in block 312 when compared in block 310, the method 300 may advance to block 316. In block 316, the privacy or restricted information may be deleted or replaced with default text or generic information. An example of default text may be "This information is unavailable" or a similar

text or message. An example of generic information may be company information of the content provider or author. If the content object is modified in block 316, the content object may be repackaged by the privacy function or P3P servlet in block 318. In block 320, the repackaged content object may be returned to the collection function or collection servlet for distribution to the requester.

[0022] Figures 4A and 4B illustrate an example of a system 400 and a sequence of operations that may be carried out by the system 400 for automatically managing privacy preferences or access to restricted information in accordance with an embodiment of the present invention. The method 100 of Figure 1 and method 300 of Figures 3A and 3B may be embodied in the system 400. The system 400 may include a server 402. The server 402 may be a web server or the like. Separate input and output (I/O) devices 406 or combination I/O devices may be coupled to the server 402 to provide an interface with the server 402 for programming purposes and to control operation of the server 402. The I/O devices 406 may include a keyboard, pointing devices, display or monitor, disk drives, optical, mechanical, or infrared I/O devices or the like.

[0023] The processor 404 may include a collection function or

program 408 or the like. The collection function 408 may be a collection servlet analogous to a Java applet for operation in a web server environment. The collection function 408 may be adapted or programmed to interrogate a plurality of content sources 410 in response to a request from a client or requester 412 for selected information. The collection function 408 may also be adapted or programmed to collect content objects 414 from the sources 410 that may correspond to the request for information. The collection function or servlet 408 may transfer or distribute selected content objects 414' to a privacy function or program 416 or the like. The collection function 408 may operate similar to that described with respect to blocks 302-306 in method 300 of Figure 3.

[0024] The privacy function 416 or program may be a Platform for Privacy Preferences Project (P3P) based servlet or the like for operation in a web server environment. The privacy function 416 or P3P servlet may parse the content object 414' to access the privacy preferences 418 of the author of the content object or to access other restriction preferences of the author or other entity providing the content object. The author's privacy preferences or other restriction preferences may be accessed or locatable via a

link, secure connection or the like, such as an xLink, similar to that described with respect to block 308 of the method 300 in Figure 3. The author's privacy preferences may be stored at a remote location from the server 402 or may be stored at another location within the server 402.

[0025] The privacy function 416 or servlet may include a compare function 420 to compare the author's privacy preferences 418 or other restriction preferences to the policies 422 of the web site or content provider. Referring also to Figure 4B, if the author's privacy preferences or other restriction preferences are consistent (block 424) with the site policies 422 from the compare function 420, the content object 426 as originally constituted or formed may be returned to the collection function or servlet 408. The original content object 426 may then be distributed or sent to the requester 412 via a network or medium 428.

[0026] If the author's privacy preferences 418 or other restriction preferences are inconsistent (block 430) when compared to the site policies 422, the privacy or restricted information or data may be deleted or replaced with default text or generic information by the privacy function or servlet 416, similar to that described with respect to block 316 of Figure 3B. The privacy function or servlet 416 may

repackage the content object 414' with the changes and the repackaged content object 432 may be returned to the collection function or servlet 408. The collection function or servlet 408 may then distribute the repackaged content object 432 to the requester 412 via the network or medium 428.

[0027] The network or medium 428 may be the Internet or a private network, such as an intranet or the like. The network or medium 428 may also be any communication network or system including by way of example, dedicated communication lines, telephone networks, and wireless data transmission systems, two-way cable systems, and customized computer networks, interactive kiosk networks or the like.

[0028] The requester 412 may access the network or medium 428 and the server 402 using a browser 434, such as a web browser or the like. The browser 434 may operate on a processor 436. Separate input and output devices 438 or combination I/O devices may be coupled to the processor 436 to permit a user or requester to operate and interface with the processor 436. The I/O devices 438 may be similar to the I/O devices 406 and may include a keyboard, pointing device, display or monitor, disk drives,

optical, mechanical, magnetic, or infrared input/output devices or the like.

[0029] Elements of the present invention, such as method 100 of Figure 1, method 300 of Figures 3A and 3B, and system 400 of Figures 4A and 4B, may be embodied in hardware and/or software as a computer program code that may include firmware, resident software, microcode or the like. Additionally, elements of the invention may take the form of a computer program product on a computer-usable or computer-readable storage medium having computer-usable or computer-readable program code embodied in a medium for use by or in connection with a system, such as system 400 of Figures 4A and 4B. Examples of such a medium may be illustrated in Figures 4A and 4B as medium 428 or I/O devices 406 and 438. A computer-usable or readable medium may be any medium that may contain, store, communicate or transport the program for use by or in connection with a system. The medium, for example, may be an electronic, magnetic, optical, electromagnetic, infrared or semiconductor system or the like. The medium may also be simply a stream of information being retrieved when the computer program product is "downloaded" through a network, such as the Internet or

the like. The computer-usable or readable medium could also be paper or another suitable medium upon which the program may be printed.

[0030] Although specific embodiments have been illustrated and described herein, those of ordinary skill in the art appreciate that any arrangement which is calculated to achieve the same purpose may be substituted for the specific embodiments shown and that the invention has other applications in other environments. This application is intended to cover any adaptations or variations of the present invention. The following claims are in no way intended to limit the scope of the invention to the specific embodiments described herein.